COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

8.

SEDUTA DI MERCOLEDÌ 27 LUGLIO 2016

PRESIDENZA DEL VICEPRESIDENTE **MASSIMO ARTINI**

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo italiani all'Estero: Misto-ALA-MAIE; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI-IDEA (Unione Sudamericana Emigrati Italiani): Misto-USEI-IDEA; Misto-FARE ! - Pri: Misto-FARE ! - Pri; Misto-Movimento PPA-Moderati: Misto-M.PPA-Mod.

PAGINA BIANCA

PRESIDENZA DEL VICEPRESIDENTE MASSIMO ARTINI

La seduta comincia alle 14.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del Consigliere militare del Presidente del Consiglio dei ministri, Generale di Divisione Carmine Masiello.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa dello spazio cibernetico, l'audizione del Consigliere militare del Presidente del Consiglio dei ministri, generale di divisione Carmine Masiello.

Saluto e ringrazio il generale Masiello per la sua presenza, oggi. Il generale è accompagnato dal colonnello Antonio Colella, ufficiale addetto all'Ufficio del Consigliere militare.

Ricordo che, dopo l'intervento del generale, darò la parola ai colleghi che intendano porre domande o svolgere osservazioni. Successivamente, il nostro ospite potrà rispondere alle domande poste. Do subito la parola al generale Masiello.

CARMINE MASIELLO, *Consigliere militare del Presidente del Consiglio dei ministri*. Innanzitutto, vorrei esprimere l'onore di essere qui davanti a questa Commissione per poter illustrare il mio ruolo e quello del mio Ufficio, nel contesto della protezione cibernetica nazionale.

L'intervento, che ho predisposto, è articolato nella seguente maniera. Farò un breve cenno al quadro normativo di riferimento della struttura nazionale, preposta alla difesa cibernetica per il nostro Paese, evidenziando il ruolo rivestito dal Consigliere militare del Presidente Consiglio dei ministri in tale contesto. Successivamente, parlerò del Nucleo per la sicurezza cibernetica (NSC) e del Nucleo interministeriale situazione e pianificazione (NISP), quale tavolo interministeriale di crisi cibernetica, entrambi organi da me presieduti, nonché dell'attività che questi svolgono per adempiere ai compiti che la norma assegna loro. Farò altresì un rapido cenno al quadro procedurale e alle attività svolte. Infine, concluderò l'intervento con alcune considerazioni.

Il contesto normativo nazionale pre-architettura *cyber* parte dalla legge n. 124 del 2007 e dalla legge n. 103 del 2012, concernenti il Sistema di informazione per la sicurezza della Repubblica, che hanno rafforzato le capacità informative d'intervento anche in ambito cibernetico. Successivamente, con il DPCM del 5 maggio 2010 sull'organizzazione nazionale per la gestione di crisi, sono state istituite le strutture per la gestione delle crisi, creando il Comitato politico strategico (CoPS) e il Nucleo interministeriale situazione e pianificazione.

Infine, il decreto legislativo n. 70 del 2012 ha definito il CERT nazionale in ambito MISE, ponendo le basi per l'architettura di sicurezza cibernetica nazionale.

Successivamente, con il DPCM del 24 gennaio 2013, anche noto come « decreto Monti », è stato attribuito al Consigliere militare del Presidente del Consiglio un

ruolo centrale di raccordo, nell'ambito dell'architettura di sicurezza cibernetica nazionale e della gestione delle crisi. Quindi, il Consigliere presiede il Nucleo per la sicurezza cibernetica e il Tavolo interministeriale di crisi cibernetica e partecipa, senza diritto di voto, alle riunioni del Comitato interministeriale per la sicurezza della Repubblica (CISR), aventi a oggetto la materia della sicurezza cibernetica.

In sostanza, come si evince, abbiamo assistito a un'evoluzione normativa, tesa all'adeguamento di compiti, strutture e procedure parallelamente all'evoluzione dello scenario *cyber*. La norma pone, in sostanza, per il Consigliere militare, un ruolo di raccordo tra i diversi organi decisionali, quale il Presidente del Consiglio dei ministri, coadiuvato dal CISR, che svolge funzioni di consulenza e di proposta alle determinazioni del Presidente in caso di crisi cibernetica, e quelli meramente di indirizzo e di coordinamento, quali il Nucleo per la sicurezza cibernetica e il Nucleo interministeriale situazione e pianificazione. Nell'ambito, quindi, di tali prerogative, l'ufficio del consigliere militare costituisce un forte catalizzatore di attività, favorendo il convogliamento delle energie verso i principali attori protagonisti dei tavoli sopra citati.

Sottolineo che l'Ufficio non svolge delle attività dirette, ma fornisce opportunità di coordinamento e raccordo, permettendo a tutti gli attori di usufruire di un ambiente interministeriale al massimo livello governativo.

Il DPCM del 2013 definisce, poi, in un contesto unitario e integrato, l'architettura istituzionale, deputata alla tutela della sicurezza nazionale, relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale, indicando, a tal fine, i compiti affidati a ciascuna componente, i meccanismi e le procedure da seguire, ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni nonché le modalità per il ripristino immediato della funzionalità dei sistemi in caso di crisi.

Il mantenimento delle funzioni vitali della società e la tutela della salute, della sicurezza e del benessere economico e sociale dei cittadini non possono prescindere dalla salvaguardia delle infrastrutture critiche nazionali ovvero di strutture e di assetti, la cui distruzione o danneggiamento impedirebbe l'esercizio di tali funzioni. L'aspettativa, infatti, che i Paesi adottino misure di adeguata sicurezza è volta principalmente a garantire la generale continuità, cosiddetta « *business continuity* », dei servizi critici forniti da tali infrastrutture, oltre che a comprendere gli effetti di eventuali eventi su altre infrastrutture o settori (*cascading effect* in anglosassone).

La protezione delle infrastrutture critiche nazionali, anche alla luce di quanto avviene in altri contesti internazionali, assume rilevanza fondamentale, quale fattore di sviluppo della sicurezza e del benessere dei cittadini, in quanto assicurare il corretto funzionamento delle infrastrutture critiche della nazione deve essere inteso non solo come un indicatore di civiltà e modernità del Paese, ma anche come fattore di buongoverno. Una politica orientata alla loro protezione, infatti, sostiene il più generale obiettivo strategico di contribuire attivamente alla sicurezza e al benessere dei propri cittadini e di quelli europei.

Tale protezione assume rilevanza fondamentale, come dicevo, anche quale fattore di sviluppo tecnologico, perché le infrastrutture moderne sono caratterizzate da settori interconnessi, interdipendenti nello spazio fisico e nel *cyber*-spazio, oltre al fatto che sono gestite attraverso una *governance*, che coinvolge attori pubblici e privati e vari livelli di autorità e responsabilità. Le reti elettriche e digitali, per esempio, sono denominatori comuni che creano interdipendenze fra i settori Telecom, aereo, ferroviario, acqua, gas, banche e finanza, solo per citarne alcuni.

Infine, assume rilevanza fondamentale anche quale fattore di sviluppo economico, in quanto gli investimenti sulle infrastrutture critiche possono sostenere, oltre allo sviluppo delle infrastrutture stesse, anche quello socio-economico delle aree, nelle quali le stesse insistono. Tali investimenti

non rappresentano meri costi, bensì un'opportunità per sostenere il sistema Paese nel complesso.

Nell'ambito dell'Unione europea, la capacità di intercettare i fondi disponibili costituisce una valida opportunità per ammodernare le infrastrutture, colmare gli eventuali *gap* tecnologici e valorizzare competenze, quindi costruire indotti ed eccellenze locali nazionali, agevolando in ultima analisi la creazione di occupazione.

I soggetti compresi nell'architettura istituzionale operano secondo un modello organizzativo funzionale, delineato con il citato decreto Monti, che persegue la piena integrazione, con le attività di competenza del Ministero dello sviluppo economico, dell'Agenzia per l'Italia digitale e delle strutture del Ministero dell'interno dedicate alla prevenzione e al contrasto del crimine informatico e alla difesa civile, nonché a quelle della protezione civile. Il decreto, quindi, riempie un vuoto normativo, cogliendo chiaramente la portata sistemica del problema della sicurezza cibernetica della nazione, delle sue infrastrutture e dei singoli cittadini e, nella sua essenzialità, si pone l'obiettivo di razionalizzare una strategia di intervento, che mira a coinvolgere i diversi attori pubblici e privati, raccordandoli in un quadro strategico nazionale, che attribuisce ciascuno i propri ruoli e le proprie responsabilità.

Gli obiettivi strategici operativi della *cyber security* italiana sono contenuti nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico e nel Piano nazionale per la protezione cibernetica e la sicurezza informatica, entrambi del 2013. Quest'ultimo, ovvero il Piano nazionale, individua priorità, obiettivi specifici e linee d'azione, per dare concreta attuazione a quanto previsto dal Quadro strategico nazionale. Entrambi i documenti sono stati elaborati dal Tavolo tecnico sul *cyber*, che opera presso il DIS e a quale partecipano i rappresentati *cyber* del CISR, dell'Agenzia per l'Italia digitale e del Nucleo per la sicurezza cibernetica.

Passo, ora, a illustrare brevemente l'architettura adottata.

La logica scelta è su tre distinti livelli di intervento. Il primo è di indirizzo politico, di coordinamento strategico e di ricerca scientifica ed è così articolato. C'è il Comitato interministeriale per la sicurezza della Repubblica, che propone al Presidente del Consiglio dei ministri l'adozione di azioni e strumenti, quali il Quadro strategico nazionale ed il Piano nazionale per la sicurezza dello spazio cibernetico, sui quali esercita l'alta sorveglianza, e, infine, elabora gli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e sicurezza informatica nazionale.

Poi, c'è l'organismo di supporto al CISR, che, come dice il nome, supporta lo svolgimento dell'attività del CISR. Infine, c'è un comitato scientifico, ossia un comitato di esperti nel campo delle discipline di interesse ai fini della sicurezza cibernetica, provenienti dalle università, da enti di ricerca, dalla pubblica amministrazione e dal settore privato, con il compito di predisporre ipotesi d'intervento, rivolte a migliorare gli standard e i livelli di sicurezza dei sistemi e delle reti. Tale comitato assicura ogni necessario contributo all'organismo collegiale di coordinamento e al Nucleo per la sicurezza cibernetica.

Il secondo livello, a carattere permanente, è rappresentato dal Nucleo per la sicurezza cibernetica, da me presieduto, con compiti di raccordo – lo ripeto – tra gli enti competenti, ai fini dell'attuazione degli obiettivi e delle linee d'azione, indicate nella pianificazione nazionale.

Il terzo livello d'intervento è rappresentato dal Nucleo interministeriale situazione e pianificazione, quale Tavolo interministeriale di crisi cibernetica, stante il suo ruolo di massimo organismo di coordinamento in situazioni di crisi, così come previsto dal DPCM del 2010. Il Tavolo cibernetico del NISP, presieduto dal Consigliere militare, è incaricato della gestione delle crisi, con il compito di curare e coordinare le attività di risposta e il ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate e mantenendo costantemente informato il Presidente del Consiglio dei ministri sulla crisi in atto.

Tale tavolo è composto da rappresentanti dei Ministeri, della pubblica amministrazione e di agenzie, a similitudine del Nucleo per la sicurezza cibernetica, con l'integrazione dei Corpo nazionale dei vigili del fuoco e della Commissione interministeriale tecnica per la difesa civile. Tali rappresentanti devono avere poteri decisionali, che impegnino le rispettive amministrazioni.

In sintesi, il terzo livello d'intervento, rappresentato dal NISP, viene attivato dal Nucleo di sicurezza cibernetica all'insorgere di una crisi ed è, pertanto, deputato alla gestione della stessa, tenendo costantemente informato il Presidente del Consiglio dei ministri.

Lo scambio delle informazioni, attività centrale per l'operatività dell'architettura di sicurezza nazionale, avviene coinvolgendo i seguenti attori: il Nucleo per la sicurezza cibernetica, quale tavolo di coordinamento delle principali amministrazioni, incluse quelle afferenti la Presidenza del Consiglio dei ministri, e il CERT, *in primis* quello nazionale, quale principale luogo di scambio informativo nell'ambito di amministrazioni pubbliche e tra queste con i privati.

Al CERT della pubblica amministrazione sono affiliate tutte le amministrazioni pubbliche e gli enti locali; invece al CERT nazionale le imprese, i cittadini e il collegamento con le paritetiche strutture di sicurezza cibernetica internazionale e con quelle della Comunità europea. Al CNAIPIC, visto quanto varato dal decreto legislativo n. 61 del 2011, spettano le funzioni di tutela delle infrastrutture informatizzate di natura critica e di rilevanza nazionale. Infine, al CERT della Difesa è demandata la funzione specifica di interfaccia con le paritetiche strutture di sicurezza cibernetica della NATO.

Passo, ora, a descrivere in dettaglio il Nucleo per la sicurezza cibernetica. Come dicevo, tale Nucleo è costituito in via permanente presso l'ufficio del Consigliere militare, a supporto del Presidente del Consiglio dei ministri, ovviamente nella materia della sicurezza dello spazio cibernetico, per gli aspetti relativi alla prevenzione e alla preparazione a eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Mi preme sottolineare che, pur trattandosi di un Tavolo interministeriale, il carattere di continuità e permanenza è assicurato dall'Ufficio attraverso il quotidiano supporto, per implementare i compiti previsti dall'articolo 9 dello stesso, per gli aspetti relativi alla prevenzione e preparazione di eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Per quest'ultimo aspetto, il Nucleo si avvale di unità per l'allertamento, che, pur collocata per ragioni amministrative presso il Ministero della difesa, opera alla luce di un definito quadro procedurale, regolamentato da attribuzioni e procedure, coordinate e da approvare dal Nucleo per la sicurezza cibernetica.

L'unità per l'allertamento ha a disposizione assetti di vario tipo, sia classificati che non classificati, che consentono di interfacciarsi, in chiaro o in modalità sicura, con le diverse amministrazioni componenti il Nucleo, favorendo, in tal modo, la condivisione tempestiva delle informazioni. L'unità di allertamento si avvale, quindi, un sistema *triage* per la valutazione degli eventi, basato su un codice di colori, dal meno grave al più grave (bianco, verde, giallo e rosso), e condiviso con tutte le amministrazioni del Nucleo, in base al quale categorizzare gli eventi rilevanti.

Lo scambio delle informazioni – evidenzio, ora, quest'aspetto – rappresenta, quindi, una delle principali attività di contrasto alle minacce cibernetiche nonché uno degli obiettivi principali del Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dal Presidente del Consiglio dei ministri nel 2013. Pertanto, nell'ambito del Nucleo per la sicurezza cibernetica, tale attività, ancorché complessa, viene condotta in modo continuo e sinergico, assumendo un ruolo preminente.

Per favorire la comprensione dei complessi flussi che si generano fra gli attori dell'architettura di sicurezza nazionale, è stato altresì redatto un *flow chart* dello

scambio delle informazioni, quale strumento che mette in sistema i diversi attori, le azioni, la direzione dei flussi e le modalità di comunicazioni in un unico documento.

Tale *flow chart* è contenuto in una pubblicazione, Procedure di condivisione dell'informazione e della diffusione degli allarmi, denominata « NSC001 », che costituisce il documento principale per il funzionamento dell'intero sistema di scambio delle informazioni. Il documento, redatto ed approvato dal Nucleo nel 2013 e revisionato nel 2015, è alla terza revisione e costituisce uno strumento estremamente flessibile, attraverso il quale il Nucleo, sulla base delle esperienze e delle evoluzioni, aggiorna le proprie capacità di scambio delle informazioni, disciplina un processo di valutazione della minaccia omogeneo e condiviso e stabilisce un sistema virtuoso di relazioni.

Dal punto di vista procedurale, completa il quadro un secondo documento, denominato « NSC002 », redatto nel 2015, che disciplina le regole di funzionamento del Nucleo per la sicurezza cibernetica, relativamente alle modalità di convocazione delle riunioni ordinarie e straordinarie, la valutazione degli eventi cibernetici, l'assunzione delle decretazioni e la dichiarazione dello stato di crisi cibernetica nazionale.

Per quanto riguarda la composizione del Nucleo, i rappresentanti appartengono al DIS, alle due Agenzie per la sicurezza, AISE e AISI, MAECI, Ministero dell'interno, Ministero della difesa, MISE, MEF, Protezione civile, Agenzia per l'Italia digitale. Inoltre, il Nucleo, per gli aspetti relativi alla trattazione di informazioni classificate, è integrato da un rappresentante dell'Ufficio centrale per la segretezza e si riunisce con cadenza periodica.

Il principale compito – lo ripeto – è quello di fungere da raccordo fra le diverse componenti dell'architettura istituzionale che intervengono, a vario titolo, in materia di sicurezza cibernetica, nel rispetto delle competenze, attribuite dalla legge a ciascuna di esse, e nel campo della prevenzione e della preparazione a eventuali situazioni di crisi.

Nello specifico, al Nucleo compete di promuove la programmazione e la pianificazione operativa, di fornire una risposta rapida ed efficace a situazioni di crisi cibernetica e, in tal senso, mantiene attiva 24 ore su 24, sette giorni su sette, l'unità per l'allertamento.

Il Nucleo valuta e promuove adeguate procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi a eventi cibernetici e per la gestione delle crisi. In tale ambito, per esempio, lo scambio con i privati avviene attraverso il CERT nazionale, di cui la dottoressa Forsi vi ha già parlato, e il CNAIPIC.

Il Nucleo acquisisce le comunicazioni circa i casi di violazioni o i tentativi di violazione della sicurezza o i casi di perdita delle integrità significative ai fini del corretto funzionamento delle reti e dei servizi. Ancora, il Nucleo promuove e coordina la partecipazione nazionale, in esercitazioni internazionali, che riguardano la simulazione di eventi di natura cibernetica. Infine, costituisce il punto di riferimento nazionale per i rapporti con le Nazioni Unite, la NATO, l'Unione europea e altre organizzazioni internazionali e Stati, fermo restando le specifiche competenze di altri dicasteri (Ministero dello sviluppo economico, Ministero degli affari esteri e della cooperazione internazionale, Ministero dell'interno e Ministero della difesa) nonché delle altre amministrazioni, così come previsto dalla normativa vigente, assicurando, comunque, in materia ogni necessario raccordo.

In materia di sicurezza cibernetica, la direttiva del Presidente del Consiglio dei ministri del primo agosto 2015, infine, oltre a stabilire che l'Agenzia per l'Italia digitale dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori *partner* del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte, dispone che il Nucleo per la sicurezza cibernetica addotti, in attuazione di quanto previsto dagli indirizzi operativi del Piano

nazionale, tutte le iniziative necessarie a potenziarne l'operatività, pianificando il pronto allineamento agli standard nazionali di riferimento.

A oggi, posso affermare che i compiti assegnati al Nucleo sono stati tutti affrontati e che hanno portato la definizione di procedure, piani e azioni, che hanno dato al Nucleo nel tempo un'identità ben definita e compiuta. A tal proposito, vorrei citare alcuni esempi significativi, in cui il Nucleo di sicurezza cibernetica è stato decisivo, nel coordinamento delle attività tra le diverse amministrazioni competenti.

Il Nucleo ha svolto, in particolare, azione di risposta, in occasione di ripetuti attacchi malevoli e rilevanti ai danni di amministrazioni dello Stato, mettendo a sistema il flusso informativo e dando notevole impulso all'attività di contrasto.

In occasione della progettazione della rete per la crisi nazionale telematica, di cui vi ha parlato l'ammiraglio Di Biase, il Nucleo ha svolto attività di raccordo tra i dicasteri competenti, determinando l'ottimizzazione delle risorse e delle tempistiche di realizzazione. Inoltre, ha promosso il confronto con altri organismi dello Stato e, appunto ieri, in occasione della riunione è stato invitato il CONSIP, sensibilizzandolo su alcune tematiche relative all'aderenza fra la contrattualistica sulla sicurezza informatica e le nuove minacce cibernetiche. Il Nucleo è stato, inoltre, punto di riferimento in alcune esercitazioni con organizzazioni internazionali dell'Unione europea e della NATO, promuovendo e testando le procedure interministeriali di gestione di eventi di natura cibernetica.

Vorrei parlare, ora, del NISP cibernetico, sul quale è necessario un discorso a parte. La problematica della gestione della crisi cibernetica, come ho detto, è assegnata al NISP in configurazione cibernetica. Quindi, il NISP si occupa della gestione di crisi e vi è poi il NISP cibernetico che si occupa delle crisi cibernetiche. A fronte di eventi cibernetici, quindi potenzialmente sfociabili in crisi cibernetiche in rapidissimo tempo, si è creata una doppia architettura, in cui chi identifica possibili eventi di crisi cibernetica nazionale è differente da chi li gestisce, li contrasta e li risolve.

A tal fine, per favorire una rapida gestione delle crisi e rimanere fedeli al dettato normativo, sono state predisposte delle procedure di raccordo tra NSC e NISP cibernetico, che permettono un rapido passaggio tra i due organismi.

Sottolineo, peraltro, che l'esperienza a livello europeo ha evidenziato che i tempi necessari per la risoluzione dei principali eventi, prettamente di spionaggio cibernetico, sono di norma dilatati e consentono un'agevole gestione anche con l'utilizzo di Tavoli diversi. Un caso a parte, invece, è quello di un attacco cibernetico propriamente detto, che colpisce infrastrutture critiche nazionali, con lo scopo di bloccare per un tempo definito i servizi essenziali. In questo caso, fa premio la rapidità di coordinamento e di una risposta sistemica, che necessita di meccanismi di risposta rapidi ed efficienti. L'attivazione del NISP deve essere, quindi, effettuata con immediatezza e in modo coordinato, al fine di consentire l'espletamento delle attività, senza soluzione di continuità e di accessibilità.

Vengo alle considerazioni finali. Le esperienze maturate da parte dell'Ufficio, in questi tre anni d'implementazione del decreto Monti del 2013 – il cosiddetto « DPCM sul *cyber* » – confermano, a oggi, la validità generale del modello scelto. Occorre, comunque, fare qualche considerazione.

Bisogna considerare, *in primis*, il rafforzamento di un solido *confidence building*: costruire un solido sentimento di fiducia è alla base della creazione di un efficace sistema di relazione fra le diverse amministrazioni. I fatti hanno dimostrato che occorre rompere la ritrosia, abbastanza naturale d'altro canto, a mettere in piazza i propri problemi ovvero rivelare alle altre amministrazioni di aver subito un attacco informatico. A onor del vero, questa non è una problematica solo italiana, ma comune a tutti i Paesi che si confrontano con la minaccia cibernetica, e rappresenta comunque un problema rilevante in contesti sociopolitici particolarmente complessi e

eterogenei, laddove le forme di Governo sono basate su sistemi burocratizzati e dispersivi.

La seconda considerazione è sul continuo adattamento del quadro procedurale. Gli sforzi effettuati, fin d'ora, nel campo delle procedure di lavoro, sono stati particolarmente intensi e tutti protesi a costituire un quadro di norme e di attività formalizzate, che permetta una perfetta sincronia fra tutti i nodi del sistema. Le procedure hanno riguardato, in modo particolare, lo scambio delle informazioni, comprese quelle dei CERT, e il funzionamento del Nucleo per la sicurezza cibernetica. La problematica sul *cyber* è in continua evoluzione, quindi le procedure devono poter adattarsi ai cambiamenti e, in tal senso, ritengo che il Nucleo svolga un ruolo fondamentale.

Infine, vorrei parlare del consolidamento della *partnership* pubblico-privati. In questo settore, occorre insistere per un sempre maggiore consolidamento dell'architettura, teso a un rafforzamento della *partnership* pubblico-privati. La condivisione dell'enorme patrimonio di conoscenza di entrambi i settori è la chiave principale per fronteggiare le sfide, sempre più complesse e globali. Il concetto che queste due realtà debbano affrontare le future sfide insieme è ormai più che consolidato, perché solo uniti si può creare un sistema di contrasto e di difesa idoneo a fronteggiare le sfide future.

Molti passi si stanno facendo anche in seno al Nucleo, protesi ad aumentare la fiducia reciproca. Sotto tale aspetto, le esercitazioni congiunte e i numerosi momenti formativi, che hanno visto la partecipazione di molte delle società private, hanno contribuito a rafforzare il comune sentimento di collaborazione. Occorre, quindi, continuare su questa strada, intensificando gli sforzi e l'occasione di reciproco scambio, con il fine di rendere le azioni sempre più fruttuose e foriere di una forte e intensa collaborazione. Vi ringrazio per l'attenzione.

PRESIDENTE. Grazie, generale. Do, ora, la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

PAOLO BERNINI. Grazie, generale, per questa spiegazione. Vorrei fare una domanda precisa. Ho letto su un articolo di giornale di tempo fa che c'è stato un attacco informatico al Ministero della difesa e Ministero degli affari esteri e della cooperazione internazionale. Vorrei sapere se erano veritiere le voci, che letto su *la Repubblica* e su *il Giornale*, di un attacco continuato di un mese e se è vero che sono stati i *cyber*-attivisti russi per rubare informazioni in ambito Nato.

In più, c'è stato, quest'anno, un convegno sul tema *cybercrime and data security*, organizzato dalla Camera di commercio americana, in cui si parla di un dato molto preoccupante: in Italia, il *cybercrime* provoca una perdita di 9 miliardi di euro all'anno. Vorrei sapere, se è possibile, quanto spende il Ministro alla difesa per il *cybercrime*.

Vorrei anche sapere se vi occupate anche di *deep web*, attraverso i vari sistemi Tor e i sistemi cosiddetti « cipolla »; non so se ne siete a conoscenza. Grazie.

PRESIDENTE. Se mi permette, generale, le faccio anch'io una domanda. Prendo uno spunto dal collega Bernini sul fatto di porre gli esempi, in cui ha funzionato al meglio, dal 2013, questo Tavolo, in caso di attivazione su minacce. La prima parte della domanda è per comprendere il numero di convocazioni ordinarie e convocazioni straordinarie, in caso di effettivo attacco.

La seconda parte è prettamente normativa. Anche a seguito di tutte le audizioni abbiamo fatto, possiamo dire che, dal DPCM del 2013, l'amministrazione ha avuto la capacità di adeguarsi per sanare eventuali sovrapposizioni. Penso, in particolare, al CNAIPIC e al CERT nazionale, sulla parte dei privati e delle infrastrutture critiche, quindi possiamo dire che i compiti sono naturalmente adeguati, a seconda dell'amministrazione.

Oltre a una revisione procedurale da parte dei Tavoli nel suo Ufficio, che porta

giovamento rispetto all'iniziale procedura, mi chiedo se c'è anche una valutazione su un'introduzione normativa diversa rispetto all'attuale, che, peraltro, non è neanche di rango primario, ma è solo regolamentare.

Infine, rispetto al rapporto tra pubblico e privato, lei parlava di ritrosia da parte delle amministrazioni nel pubblicare informazioni relativamente ad attacchi, perché chi è attaccato solitamente cerca di risolvere il danno e non farlo sapere a nessuno. Questo vale anche, in particolare, per i privati, che possono trattare anche con la pubblica amministrazione. Mi chiedo se c'è la volontà di introdurre, anche a livello di norma primaria e su spinta del Governo, modalità come quelle, per esempio, degli Stati Uniti, oppure dell'esperienza olandese.

Volendo citarle entrambe: negli Stati Uniti, è necessario rendere pubblico, da parte delle imprese, l'attacco, cosa che è molto importante, anche per aziende, che possono avere delle fluttuazioni dal punto di vista azionario rispetto a quei terribili attacchi, mentre l'Olanda – per fare un ragionamento su un *partner* europeo – ha un approccio sicuramente meno conservativo. Io ho avuto l'opportunità di parlare con alcuni responsabili di *cyber* in Olanda, che mi dicevano che il fatto che loro possano contrattaccare, in maniera normata, a un eventuale attacco porta una naturale deterrenza, quindi a una riduzione di attacchi da parte di altri *hacker* o attori malevoli sul settore del *cyber*. Grazie.

DANIELE MARANTELLI. La ringrazio, generale. Non so se lanciare un *assist* o fare un autogol con questa domanda, ma comunque la faccio in questi termini.

In precedenti audizioni sullo stesso tema, ci è stato detto che esiste una sproporzione evidente tra quanto il nostro Paese impegna nel campo (150 milioni di euro, pressappoco) e i Paesi europei a noi vicini, come la Germania e la Francia, che, invece, impegnano intorno al miliardo di euro. Questo *gap* evidente è così insuperabile da garantire, comunque, al nostro Paese elevati margini di sicurezza in questo campo ?

Questa è la prima domanda, mentre la seconda è a questa conseguente. Siete in grado di valutare se gli attacchi di questo tipo possano procurare danni anche al nostro sistema produttivo, ovvero al nostro capitale fatto di brevetti e di realtà preziose che sono all'interno delle medie imprese italiane e, a volte, anche delle piccole, non in grado autonomamente di tutelare sempre questo bene, che, per me, costituisce un capitale formidabile. Grazie.

PRESIDENTE. Do la parola al generale Masiello per la replica.

CARMINE MASIELLO, *Consigliere militare del Presidente del Consiglio dei ministri*. Grazie per le domande. Fermo restando che mi riservo di dare delle risposte scritte e compiute su tutte e tre le questioni, in merito all'attacco *cyber* alla Difesa, ritengo che forse ne possa parlare più completamente il dicastero competente. Sicuramente la tematica è stata trattata a livello di Nucleo e così rispondo anche alla domanda dell'onorevole Artini.

Questo non è stato l'unico caso: infatti, c'è stato anche un altro caso che ha interessato un'altra amministrazione, che è stato prontamente gestito a livello di Nucleo, dove sono state raccordate le informazioni e sono state individuate le soluzioni, per porre fine a questa attività. Con questo voglio dire che, in entrambi i casi, che sono forse i più eclatanti tra quelli all'attenzione del Nucleo, il Nucleo e l'architettura istituzionale hanno risposto prontamente, nelle loro diverse forme. Da questo punto di vista, posso affermare che l'architettura funziona, perché in due casi l'abbiamo testata e in entrambi ha risposto come doveva, in ognuna per la parte di competenza.

Il Nucleo svolge – lo ripeto – funzioni di raccordo, quindi convoca al Tavolo gli aventi causa e facilita soprattutto lo scambio di informazioni fra tutti, nonché l'individuazione delle soluzioni. Non si è mai arrivati, a oggi, a una situazione di crisi cibernetiche vere e proprie, che abbiano comportato l'attivazione del NISP cibernetico, quindi queste sono tutte situazioni che

sono state gestite senza attivare la situazione di crisi cibernetica.

Riguardo ai dati su quanto spende il Ministero della difesa, posso dire che li fornirò per iscritto.

Per quanto riguarda la domanda relativa la sproporzione esistente fra quanto si spende nei Paesi, io rispondo ovviamente per il Nucleo per la sicurezza cibernetica, quindi non posso rispondere su questo, come può capire.

Siamo in grado, se le imprese si rivolgono al CERT, di gestire anche gli attacchi. Quello che vorrei sottolineare è che si tratta di un problema culturale, di cui si è ampiamente dibattuto anche nelle precedenti audizioni di questa indagine conoscitiva, e che l'investimento per l'impresa di qualsiasi dimensione nel mondo *cyber* deve far parte dell'investimento dell'impresa e non può più essere considerato un qualcosa *a latere*, perché, oggi, è un aspetto imprescindibile dell'attività imprenditoriale.

Per quanto riguarda, onorevole Artini, la questione delle sovrapposizioni, posso dire che si tratta di una cosa che ho notato guardando l'organizzazione istituzionale. Fermo restando che, a mia conoscenza, non vi sono modifiche normative di origine governativa per quanto riguarda l'architettura, rilevo soltanto che la ridondanza in taluni settori – parlo da militare – può essere, a volte, una garanzia di continuità di funzionamento, infatti noi comandanti diciamo che è sempre meglio avere una riserva, quindi, a volte, è meglio avere due canali di ingresso anziché uno solo. Grazie.

PRESIDENTE. Ringrazio il generale Masiello per l'esauriente relazione, nonché per la presentazione informatica che ci ha consegnato, di cui autorizzo la pubblicazione in allegato al resoconto stenografico dell'audizione (*vedi allegato*).

Dichiaro conclusa l'audizione.

La seduta termina alle 14.40.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. RENZO DICKMANN

Licenziato per la stampa
il 23 settembre 2016

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

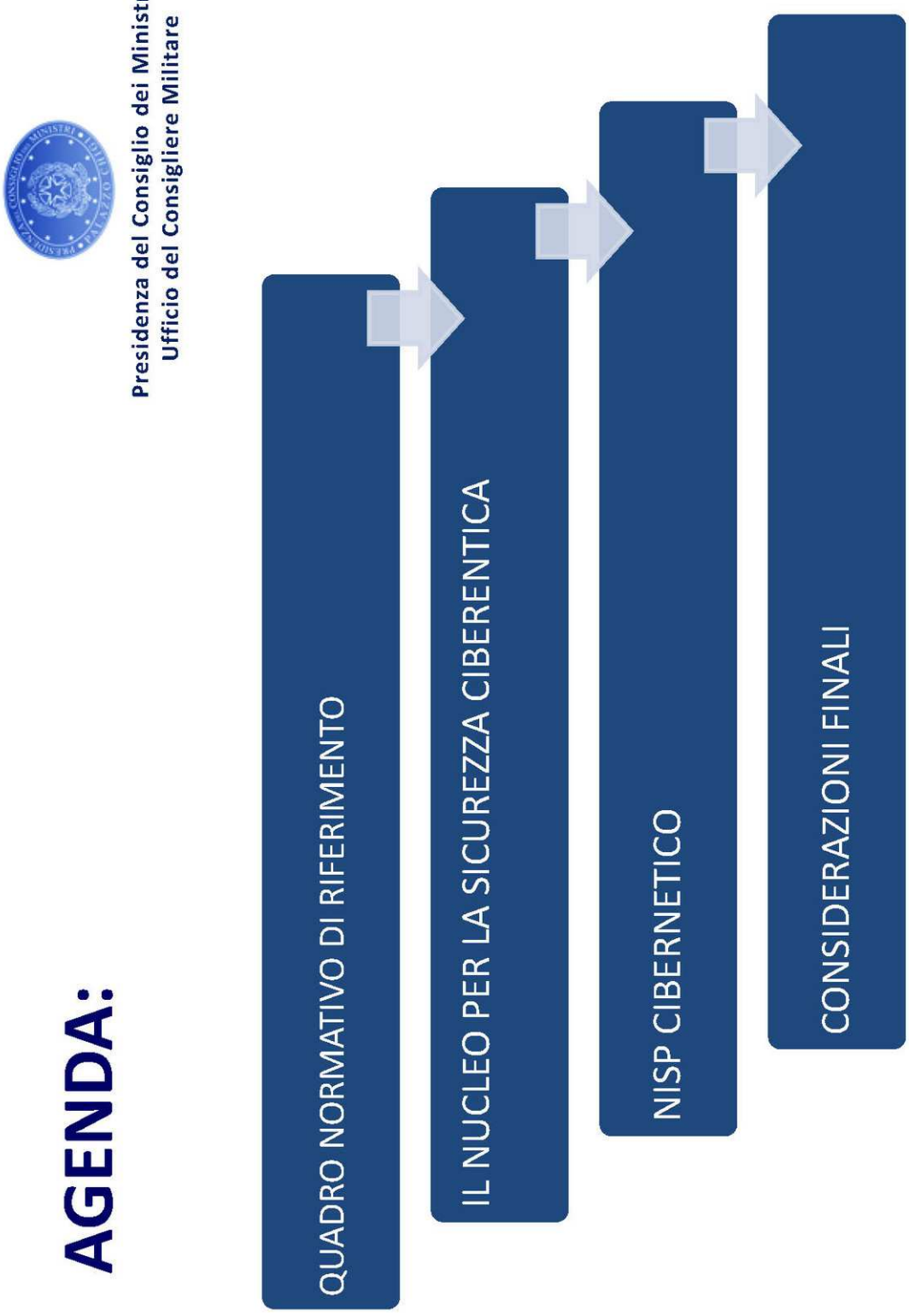
Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

CAMERA DEI DEPUTATI
IV COMMISSIONE – DIFESA

«Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico»

IL NUCLEO PER LA SICUREZZA CIBERNETICA

Roma, 27 luglio 2016


Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare
AGENDA:
QUADRO NORMATIVO DI RIFERIMENTO
IL NUCLEO PER LA SICUREZZA CIBERENTICA
NISP CIBERNETICO
CONSIDERAZIONI FINALI

QUADRO NORMATIVO DI RIFERIMENTO

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

RIFERIMENTI NORMATIVI

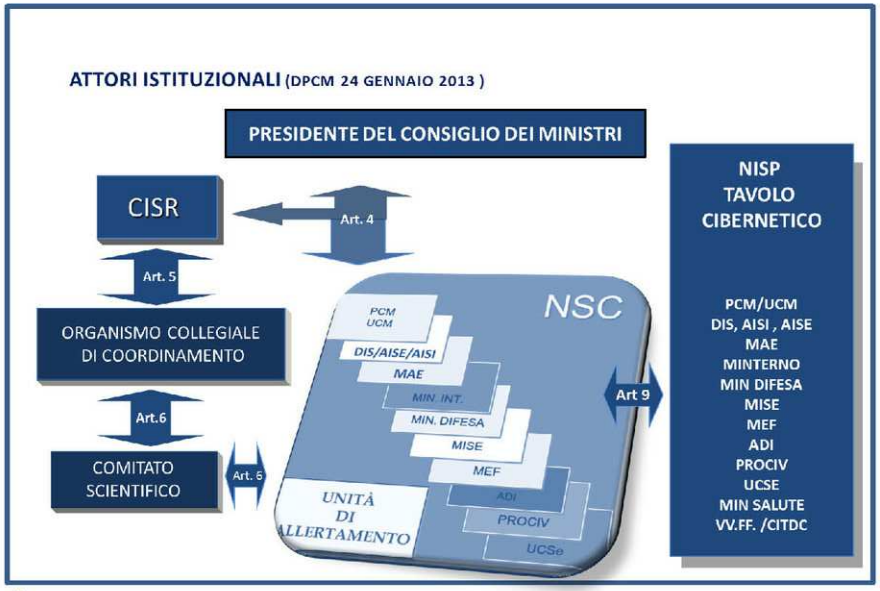
CONTESTO LEGISLATIVO NAZIONALE (PRE-ARCHITETTURA CYBER)

QUADRO NORMATIVO DI RIFERIMENTO

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

DPCM 24 GENNAIO 2013


DECRETI PRESIDENZIALI



"Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

QUADRO NORMATIVO DI RIFERIMENTO

La sicurezza dello spazio cibernetico a protezione delle infrastrutture strategiche

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

QUADRO NORMATIVO DI RIFERIMENTO

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

QUADRO STRATEGICO E PIANO NAZIONALE

…CON QUESTI DUE STRUMENTI L'ITALIA SI DOTA DI UNA **STRATEGIA** ATTORNO ALLA QUALE **COORDINARE** GLI SFORZI PER RAFFORZARE LA NOSTRA CAPACITA' DI FARE SQUADRA PER GUARDARE CON FIDUCIA ALLE SFIDE DI SICUREZZA DELLO SPAZIO CIBERNETICO…

QUADRO NORMATIVO DI RIFERIMENTO

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

Cosa fa l'Italia

DPCM 24 GENNAIO 2013


DECRETI PRESIDENZIALI

"Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

individua tre livelli dell'architettura cyber nazionale:

- **1° Livello**: indirizzo politico e coordinamento strategico;
- **2° Livello:** supporto, a carattere permanente;
- **3° Livello** : gestione della crisi (coordinamento funzioni di risposta e ripristino delle funzionalità dei sistemi

stabilisce una progressività nella definizione del quadro strategico nazionale in materia di sicurezza informatica

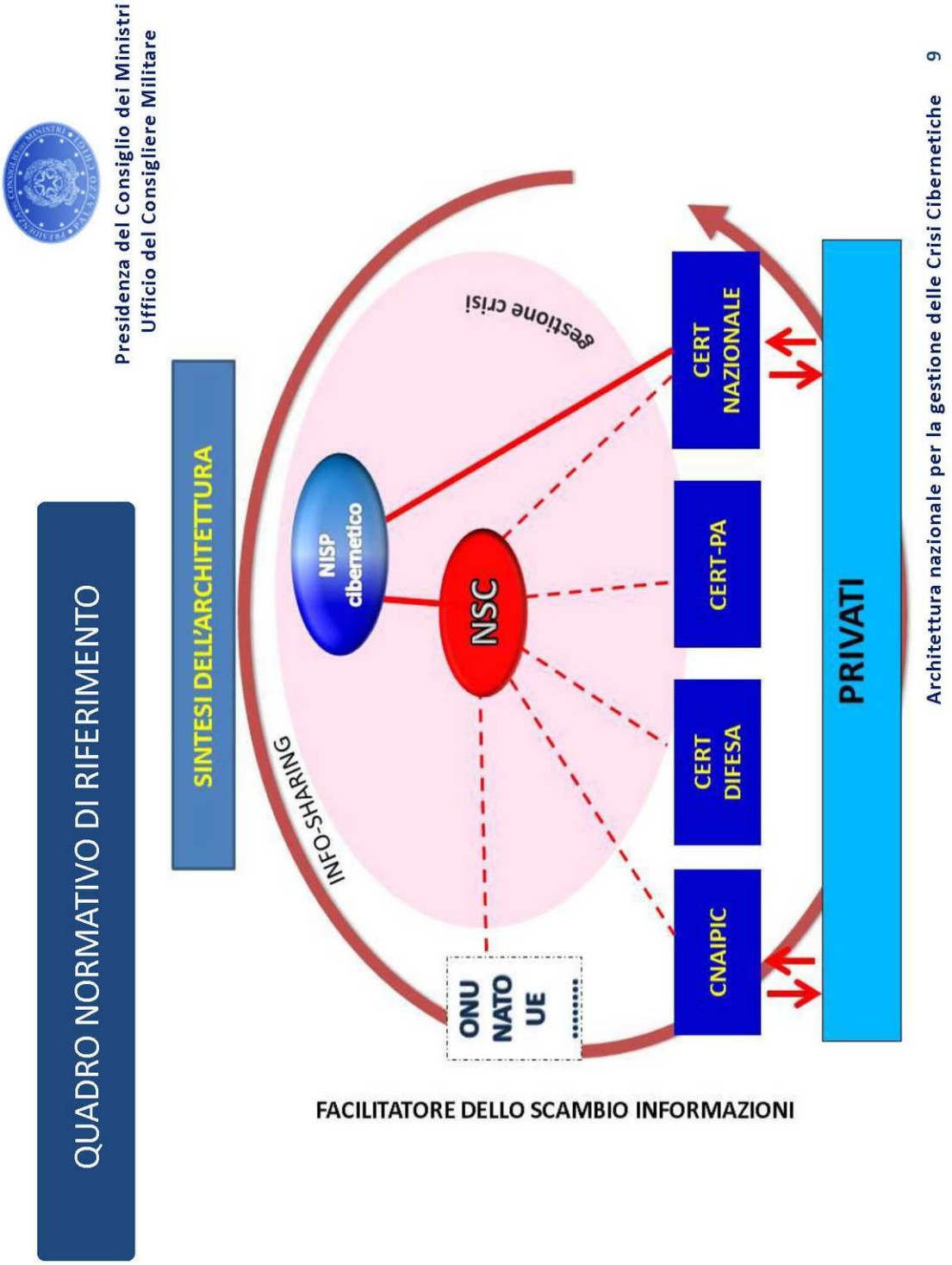
prevede la composizione di un **Nucleo di Sicurezza Cibernetica** e di un **"Tavolo interministeriale di crisi cibernetica"**, per la gestione delle crisi (mentre per gli aspetti tecnici di *computer emergency response*, si avvarrà del CERT nazionale istituito presso il Ministero dello Sviluppo Economico.

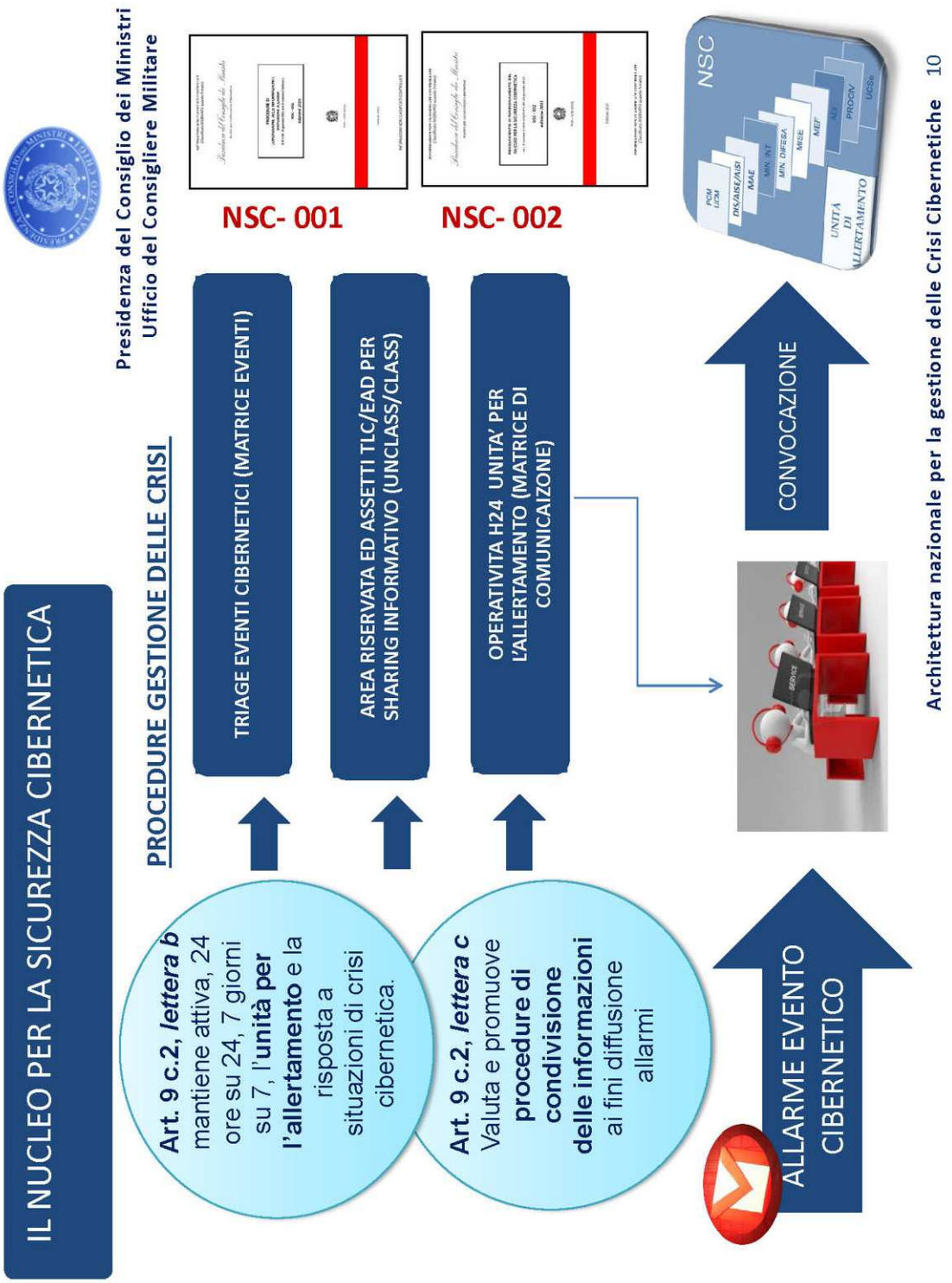
QUADRO NORMATIVO DI RIFERIMENTO

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

ATTORI ISTITUZIONALI (DPCM 24 GENNAIO 2013)

Architettura nazionale per la gestione delle Crisi Cibernetiche 8


Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare
QUADRO NORMATIVO DI RIFERIMENTO
SINTESI DELL'ARCHITETTURA
gestione crisi
NISP cibernetico
NSC
CERT NAZIONALE
CERT-PA
CERT DIFESA
CNAIPIC
PRIVATI
ONU NATO UE .....
INFO-SHARING
FACILITATORE DELLO SCAMBIO INFORMAZIONI
Architettura nazionale per la gestione delle Crisi Cibernetiche 9


IL NUCLEO PER LA SICUREZZA CIBERNETICA
Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare
PROCEDURE GESTIONE DELLE CRISI
NSC- 001
NSC- 002
TRIAGE EVENTI CIBERNETICI (MATRICE EVENTI)
AREA RISERVATA ED ASSETTI TLC/EAD PER SHARING INFORMATIVO (UNCLASS/CLASS)
OPERATIVITA H24 UNITA' PER L'ALLERTAMENTO (MATRICE DI COMUNICAIZONE)
NSC
PCM UCM
DIS/AISE/AISI
MAE
MIN. INT
MIN. DIFESA
MISE
MEF
UNITÀ DI ALLERTAMENTO
PROCIV
UCSe
CONVOCAZIONE
Art. 9 c.2, lettera b mantiene attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica.
Art. 9 c.2, lettera c Valuta e promuove procedure di condivisione delle informazioni ai fini diffusione allarmi
ALLARME EVENTO CIBERNETICO
Architettura nazionale per la gestione delle Crisi Cibernetiche 10

IL NUCLEO PER LA SICUREZZA CIBERNETICA

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

NSC – CRISI CIBERNETICA

Art. 9 c.3, b) valuta se l'evento assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale

Art. 9 c.3, b) se l'esigenza richiede assunzione di decisioni coordinate in sede interministeriale viene dichiarata la **situazione di crisi cibernetica**

- DICHIARAZIONE SITUAZIONE CRISI CIBERNETICA NAZIONALE
- ATTIVAZIONE NISP CIBERNETICO
- TEMPESTIVA COMUNICAZIONE AL PCM

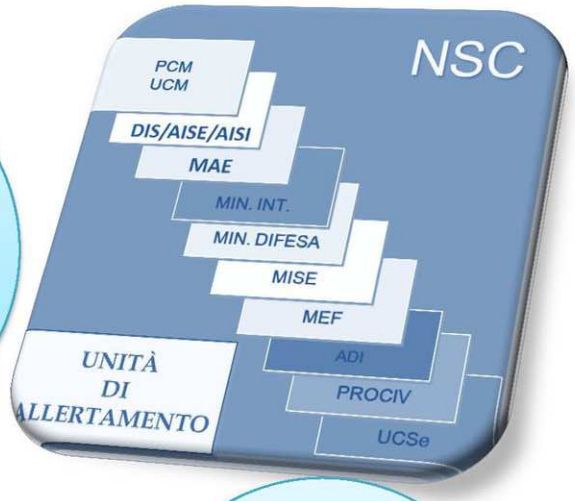
- FOLLOW ON (MONITORAGGIO)
- GESTIONE EVENTO (LIVELLO DICASTERIALE)

IL NUCLEO PER LA SICUREZZA CIBERNETICA

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

NUCLEO PER LA SICUREZZA CIBERNETICA (FUNZIONI)

Art. 9 c.2, *lettera f* costituisce **punto di riferimento nazionale** per i rapporti con l'ONU, la NATO, l'UE, altre organizzazioni internazionali ed altri Stati



Art.9 c.2, *lettera a* promuove la **programmazione** e la **pianificazione operativa** della **risposta** a situazioni di crisi

Art. 9 c.2, *lettera e* promuove e coordina **esercitazioni** interministeriali di eventi di natura cibernetica

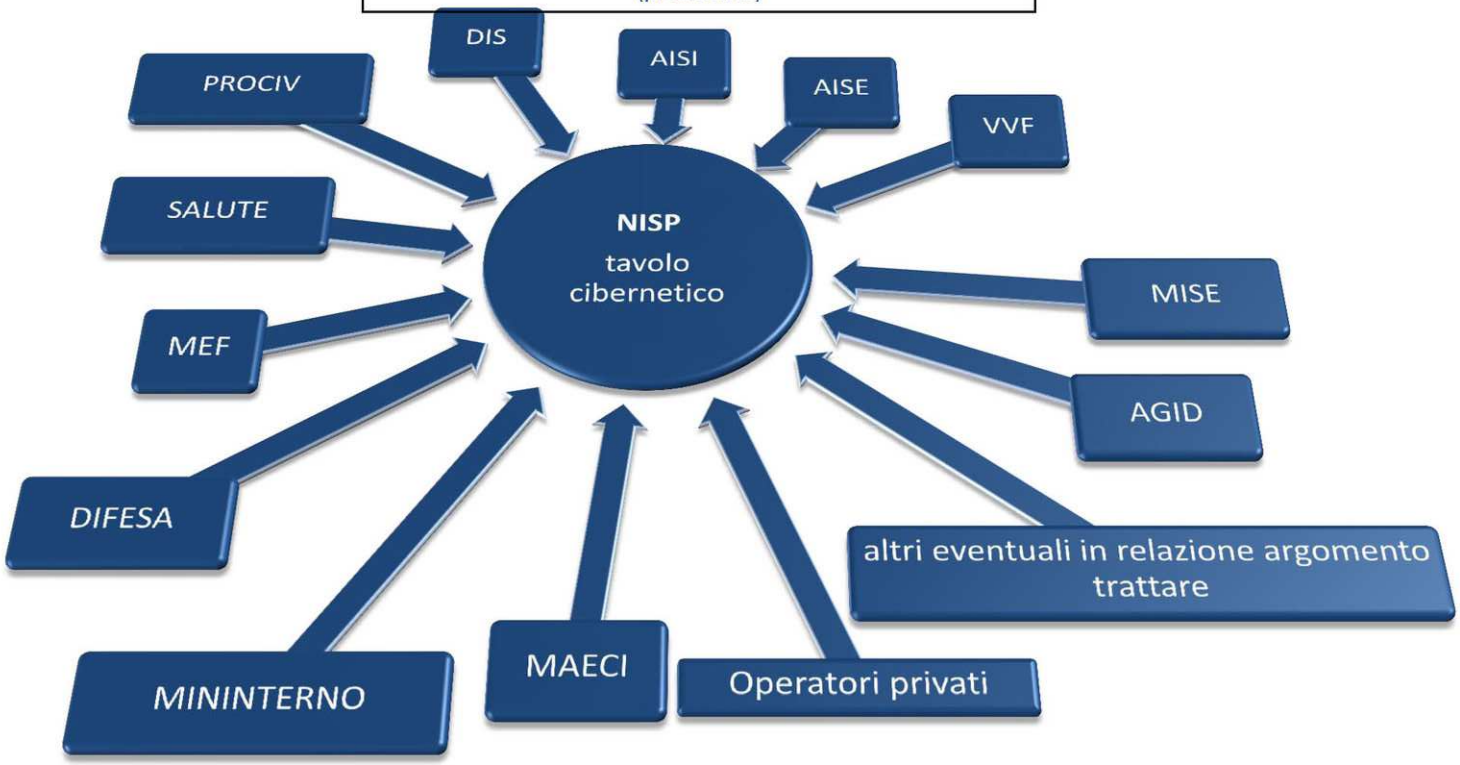
Art. 9 c.2, *lettera c* Valuta e promuove **procedure di condivisione delle informazioni** ai fini diffusione allarmi

Art. 9 c.2, *lettera b* mantiene attiva, 24 ore su 24, 7 giorni su 7, l'**unità per l'allertamento** e la risposta a situazioni di crisi cibernetica.

NISP CIBERENTICO

NISP – TAVOLO CIBERNETICO (COMPOSIZIONE)

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare



Architettura nazionale per la gestione delle Crisi Cibernetiche 13

CONSIDERAZIONI FINALI

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

- Rafforzamento di un solido *confidence building*: Costruire un solido sentimento di fiducia;
- Continuo adattamento del quadro procedurale;
- Consolidamento della partnership pubblico - privato

Presidenza del Consiglio dei Ministri
Ufficio del Consigliere Militare

CAMERA DEI DEPUTATI
IV COMMISSIONE – DIFESA

«*Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico*»

IL NUCLEO PER LA SICUREZZA CIBERNETICA

Roma, 27 luglio 2016

PAGINA BIANCA

17STC0018650